

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH APPLE ID

iclarke16431@icloud.com AND APPLE ID

johnlevy213@yahoo.com THAT IS STORED AT PREMISES
CONTROLLED BY APPLE, INC.

Case No.

2:21-mj-28

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 666(a)(1)(B)	Bribery
18 USC 1343, 1346	Wire Fraud
18 USC 1951	Extortion

The application is based on these facts:
See affidavit

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet

Sworn to before me and signed in my presence. by video

Date:

1/20/2021

City and state:

Columbus, OH

Elizabeth Preston Deavers, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
APPLE ID lclarke16431@icloud.com AND
APPLE ID johnlevy213@yahoo.com THAT
IS STORED AT PREMISES CONTROLLED
BY APPLE, INC.

Case No.

2:21-mj-00028

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Bryan Lacy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California, 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since March 2010. I am currently assigned to the Cincinnati Division, where I investigate among other things, violent crimes, weapons violations, money laundering, public corruption, and fraud. I have received specialized training in investigating violations of federal statutes from the FBI. I have conducted physical and electronic surveillance, debriefed confidential human sources, and

participated in numerous arrests. In addition, I have written, sworn to, and executed numerous search warrant affidavits.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 666, 1343, 1346 (bribery, wire fraud) and 18 U.S.C. § 1951 (extortion) have been committed by John Levy. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Federal law prohibits public officials—including government contractors—from receiving or agreeing to receive anything of value in exchange for an official act. *See* 18 U.S.C.

§§ 666¹, 1343, 1346. Federal law also prohibits obtaining property from another, with his consent, induced by wrongful use of fear (including fear of economic harm) or under color of official right. *See* 18 U.S.C. § 1951.

7. On or about September 20, 2019, a cooperating witness, hereinafter referred to as “CW1”, was arrested by former Steubenville Police Officer John Levy following a car stop in Steubenville, which is in the Southern District of Ohio. In the incident report, Officer Levy reported that he “conducted a probable cause search of the vehicle recovering approximately 11.2 grams of Crack-Cocaine in a bag that was field tested with a presumptive positive result for cocaine base and 16 packages of sealed marijuana and 2 jars of sealed marijuana.”

8. A review of the patrol vehicle dash camera video recording of the incident was made by your affiant. On the video, Officer Levy can be seen searching CW1’s vehicle. Officer Levy removed a black bag from the back seat of CW1’s vehicle, searched the bag, and eventually placed the bag inside the trunk of his patrol vehicle.

9. On or about December 4, 2019, an indictment was filed by the State of Ohio, Jefferson County, charging CW1 with possession of twelve grams of cocaine, in violation of Sections 2925.11(A) and 2925.11 (C)(4)(c) of the Ohio Revised Code, it being a Felony of the Third Degree.

10. The suspected cocaine was submitted to the Ohio Bureau of Criminal Investigation Laboratory Division for testing. On or about December 5, 2019, according to a

¹ 18 U.S.C. § 666, stipulates that that the organization, government, or agency receives, in any one year period, benefits in excess of \$10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, or other form of Federal assistance. The Steubenville Police Department is a local government agency that received federal assistance in excess of \$10,000 in a one year period.

supplement report by the Steubenville Police Department, the results of the laboratory test showed the submitted substance was cocaine and weighed about 8.84 grams, without the bag.

11. On or about January 16, 2020, a second cooperating witness, hereinafter referred to as "CW2", was arrested by the Jefferson County Drug Task Force following a narcotics investigation. While in custody, CW2 was given his Miranda warnings and agreed to waive his Fifth Amendment right to counsel. CW2 gave a statement that CW1 "got caught with fifty some grams" by Officer Levy. CW2 said "Levy got rid of everything, but he was supposed to get it all the way down to under 10 grams, and I think it ended up being 14 grams." CW2 added "There's tapes of it and everything." CW2 said CW1 also had about 60 bags of marijuana when arrested by Officer Levy.

12. After learning of the allegations made by CW2, on or about May 19, 2020, the FBI contacted defense counsel for CW1 to asked if CW1 would be willing to speak with the FBI regarding the allegations against Officer Levy. Following the FBI request to speak with CW1, defense counsel for CW1 sent to law enforcement an audio recording purportedly of a conversation between CW1 and Officer Levy.

13. A review of the audio recording was made by law enforcement. Detectives with the Steubenville Police Department and the Jefferson County Sheriff's Office listened to the audio recording and confirmed that one of the male voices on the recording was Officer Levy. Officer Levy can be heard discussing with CW1 getting CW1's charges reduced from a third-degree felony to a fourth-degree felony and getting a sentence of probation instead of jail time. Officer Levy said "I'm going to need another two on that eight, because that's clean. That's clean. No mother-fucking jail time at all. So, you should be in, so, you should be doing ten

years.” Your affiant believes Officer Levy asked CW1 for \$10,000 in exchange for getting CW1’s charges reduced.

14. On or about May 29, 2020, CW1, along with his attorney, met with law enforcement regarding CW1’s arrest by Officer Levy and the subsequent audio recording with Officer Levy. CW1 stated that inside the book bag that was seized by Officer Levy on September 20, 2019 was over 20 grams of cocaine, approximately 20 to 22 sealed bags of marijuana, and approximately two jars of marijuana. According to CW1, the amount of drugs in the book bag was greater than the amount of drugs reportedly seized by Officer Levy.

15. CW1 stated that soon after getting arrested by Officer Levy, CW1 had asked a third-party, hereinafter referred to as “S.J.”, to initiate contact with Officer Levy on his behalf. S.J. was a mutual acquaintance of both CW1 and Officer Levy. S.J. tried to contact Officer Levy several times using the Facebook Messenger application on her cell phone. At first Officer Levy didn’t respond, but then S.J. sent dollar sign emojis, which Office Levy immediately responded to.

16. CW1 stated that the audio recording sent to law enforcement, as mentioned in paragraph 11, was made on or about September 23, 2019. CW1 had covertly recorded Officer Levy during a FaceTime conversation with Officer Levy on S.J.’s cell phone. CW1 stated that Officer Levy asked CW1 for \$10,000 in exchange for getting CW1’s offense reduced to a fourth-degree felony. CW1 did not give Officer Levy any money, because he was hoping the charges were going to get dropped at a suppression hearing in his case.

17. On or about August 25, 2020, law enforcement interviewed S.J. regarding his/her interactions with Officer Levy and CW1. S.J. stated that he/she received a call from CW1 around 11:30 p.m. on the same day CW1 was arrested by Officer Levy, September 20, 2019. S.J. agreed

to meet with CW1 later that evening at a restaurant in Steubenville, Ohio. At the restaurant, CW1 asked S.J. to contact Officer Levy for CW1. S.J. had known Levy for approximately four or five years. According to S.J., the “word on the street” was that Officer Levy would take payment for doing favors for individuals facing criminal charges.

18. Using his/her cell phone, S.J. called Officer Levy, telephone number 740-381-4314. Once S.J. got ahold of Officer Levy on the phone, he/she gave the phone to CW1 so CW1 could have a phone conversation with Officer Levy. S.J. did not hear details of the conversation between CW1 and Officer Levy, however S.J. understood CW1 wanted to ask Officer Levy to help him regarding his arrest.

19. S.J. stated that in the days following CW1’s arrest, CW1 called officer Levy, telephone number 740-381-4314, multiple times using S.J.’s phone. Communications with Levy were mostly through telephone calls to and from Levy’s phone number 740-381-4314. S.J. didn’t have any recollection of communicating with Levy through Facebook Messenger.

20. Telephone number 740-381-4314 was a Sprint account established November 13, 2017, subscribed to by John Levy, 1419 Orchard Street, Steubenville, Ohio. A review of the toll records for telephone number 740-381-4314 from November 18, 2017 to May 21, 2020 revealed approximately 100 calls between S.J.’s phone and Levy’s phone starting on or about September 20, 2019 at approximately 10:50 p.m. CW1 was arrested by Officer Levy on September 20, 2019 at approximately 6:38 p.m. S.J. stated that S.J. and CW1 began calling Officer Levy on the same day.

21. On or about August 21, 2020, a request was submitted to Apple to preserve for 90 days information related to telephone number 740-381-4314. Apple confirmed receipt of the preservation request and assigned case number 20371670. On November 18, 2020 the request was extended for an additional 90 days.

22. A review of the account details records from Apple revealed that telephone number 740-381-4314 was associated with John Levy, Apple ID lclarke16431@icloud.com created on October 14, 2012 and John Levy, Apple ID johnlevy213@yahoo.com created on May 29, 2020.

INFORMATION REGARDING APPLE ID AND iCloud²

23. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

24. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

² The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at <https://support.apple.com/kb/PH26502>.

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

25. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

26. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to

access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

27. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

28. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service,

including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

29. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

30. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and

videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud Drive. Some of this data is stored on Apple’s servers in an encrypted form but can nonetheless be decrypted by Apple.

31. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

32. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

33. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs,

documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

34. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

35. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

36. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

37. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.


CONCLUSION

38. Based on the forgoing, I request that the Court issue the proposed search warrant.

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

40. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,


Bryan Lacy
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on _____, 2021.



ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID lclarke16431@icloud.com and Apple ID johnlevy213@yahoo.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California, 95014.

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from September 20, 2019 to May 29, 2020, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from September 20, 2019 to May 29, 2020, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within fourteen days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 666, 1343, 1346 (bribery, wire fraud) and 18 U.S.C. § 1951 (extortion) involving John Levy since September 20, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Any and all communications between John Levy, S.J., CW1 and any other parties relating to the crime under investigation;
- b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- e. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be

conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.